#3

Fig. 1

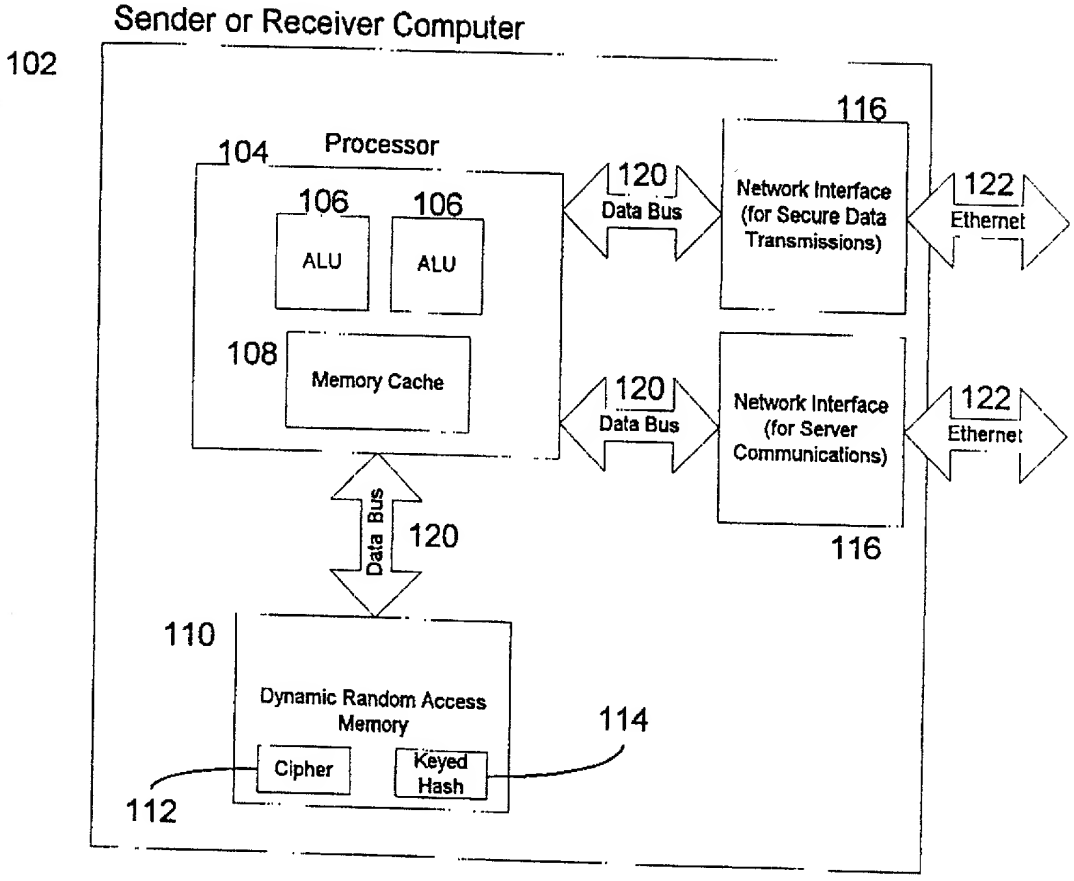
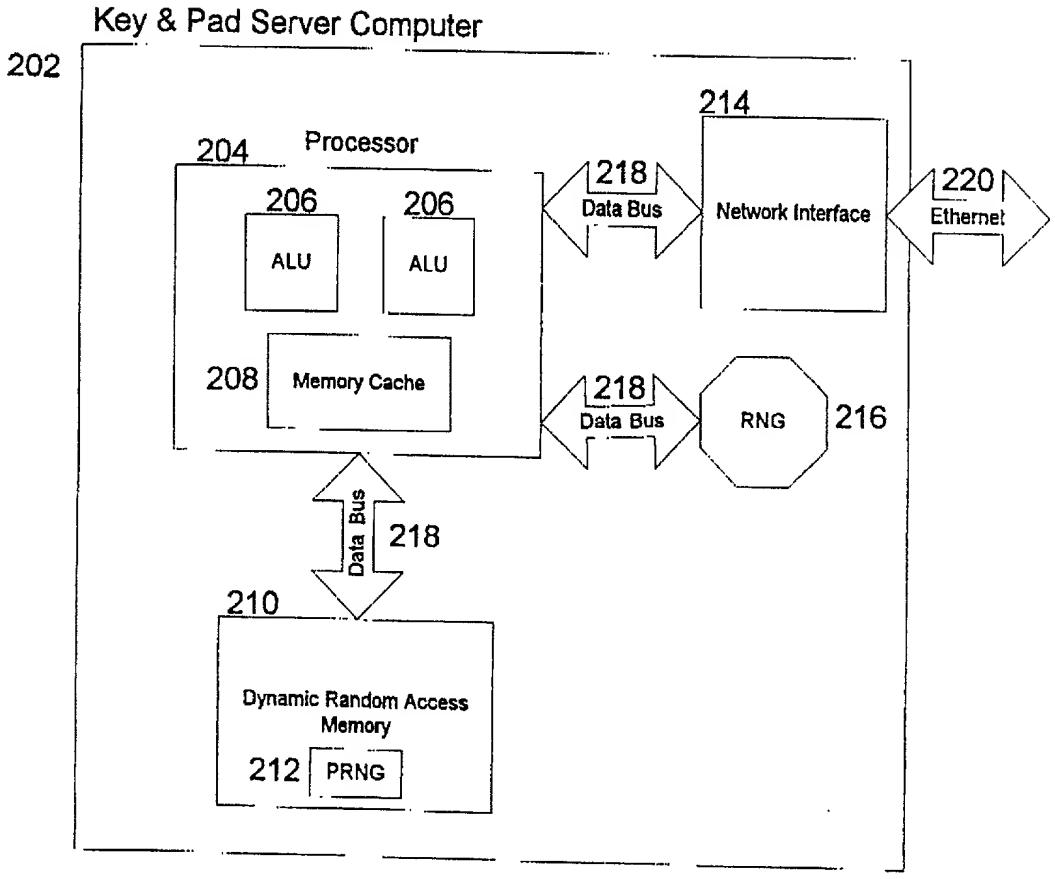
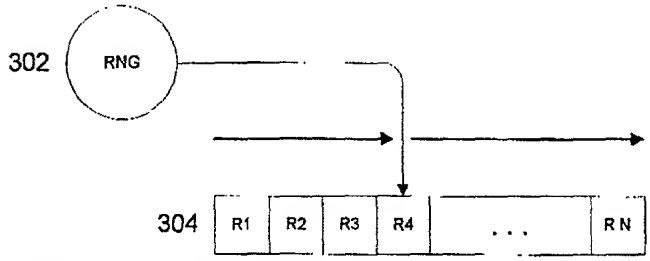

Sender or Receiver Computer
102
104
Processor
106
ALU
106
ALU
108
Memory Cache
120
Data Bus
116
Network Interface
(for Secure Data
Transmissions)
122
Ethernet
120
Data Bus
Network Interface
(for Server
Communications)
122
Ethernet
116
Data Bus
120
110
Dynamic Random Access
Memory
Cipher
Keyed
Hash
114
112

Fig. 2


Key & Pad Server Computer
202
204
Processor
206
ALU
206
ALU
208
Memory Cache
210
Dynamic Random Access Memory
212
PRNG
218
Data Bus
214
Network Interface
220
Ethernet
218
Data Bus
RNG
216
218
Data Bus

Simple Mechanism of Generating a Random Permutation of a Sequence of Unique Numbers from 0 to N

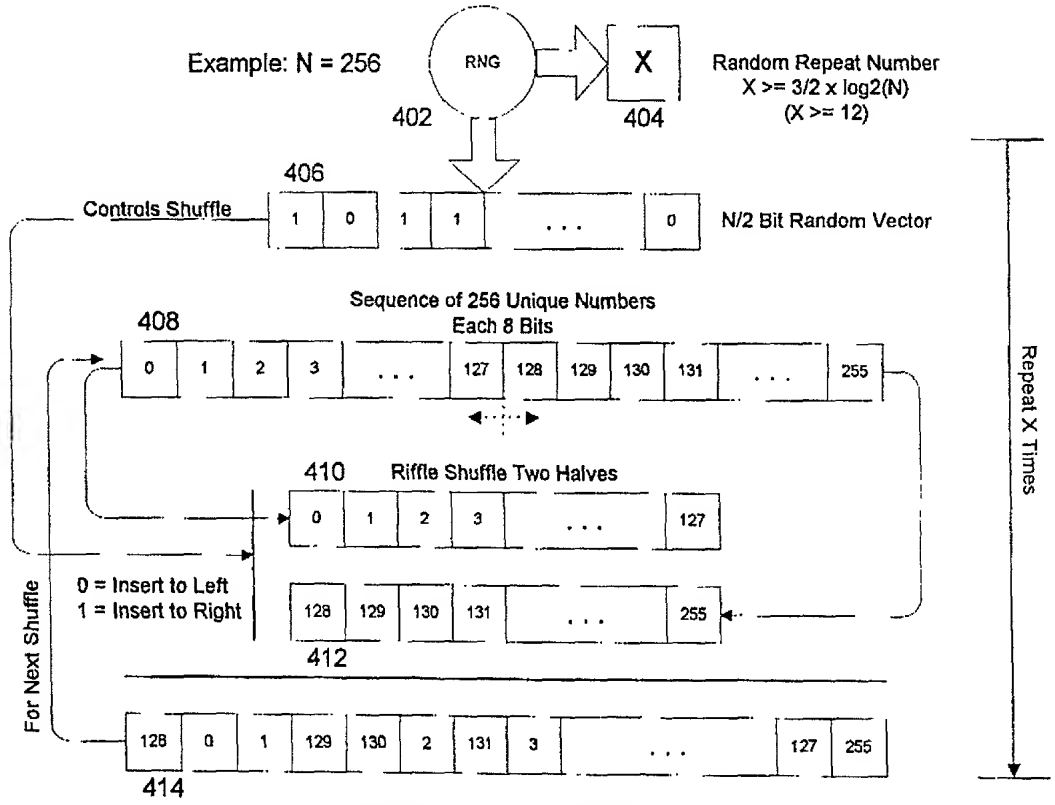
Fig. 3



Random Permutation of a Sequence of N Unique Numbers (0 to N-1 Values)
Each of Log2(N) Bits

Fig. 4

Near Perfect Riffle Shuffle Mechanism of Generating a Random Permutation of a Sequence of Unique Numbers from 0 to N.



Randomly Shuffled Sequence of 256 Unique Numbers
Each 8 Bits

Fig. 5 Randomly Permutating a Sequence of Numbers

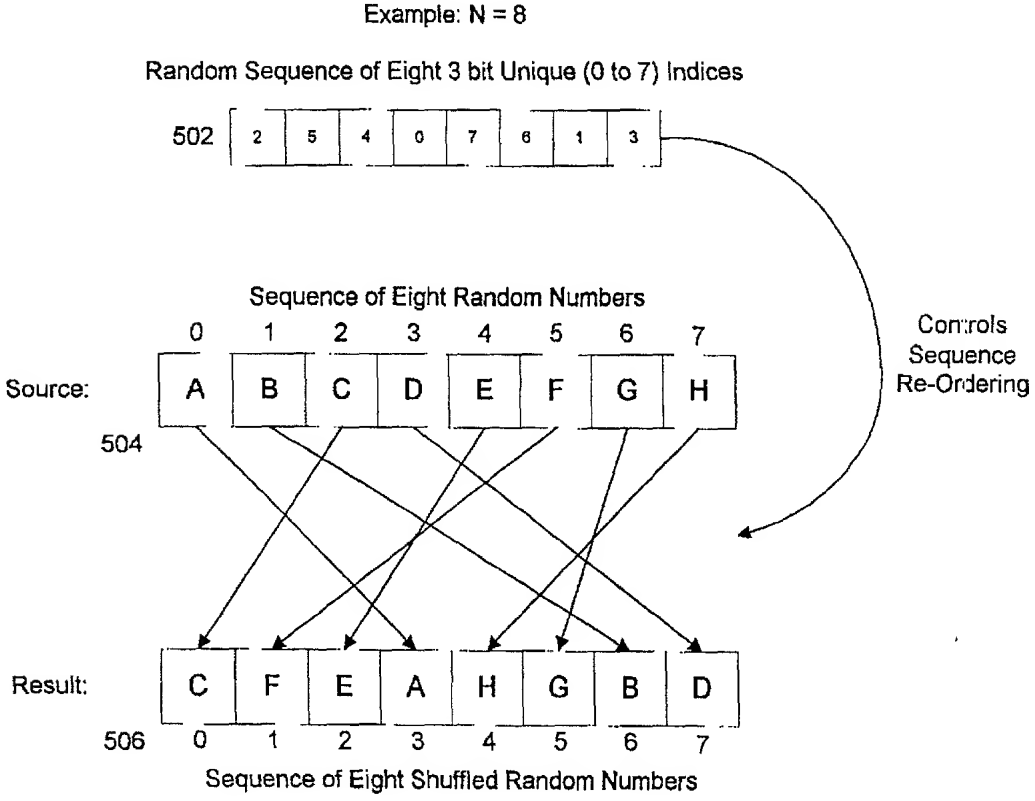
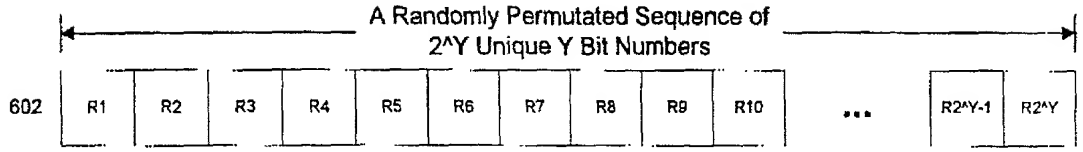
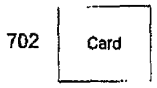


Fig. 6 Key or Seed Data Structure

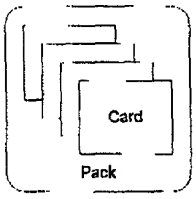


where Y = 6, 7, or 8

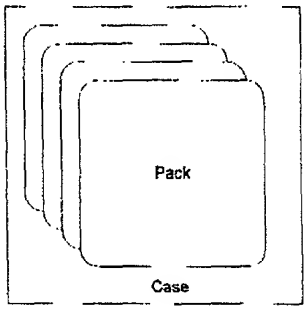
Fig. 7 Unit Sizes Used For Partitioning Random Permutations



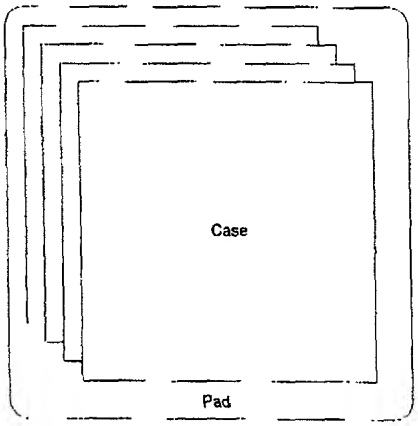
1 Card = 2^U Bytes, where U = 0, 1, 2, 3, or 4 (i.e. 1, 2, 4, 8, or 16 Bytes)



1 Pack = 2^V Cards, where V = 6, 7, 8 or more.



1 Case = 2^W Packs, where W = 6, 7, 8 or more.



1 Pad or Pool = 2^X Cases, where X = 6, 7, 8 or more

Fig. 8 Flow Chart for Nested Shuffle

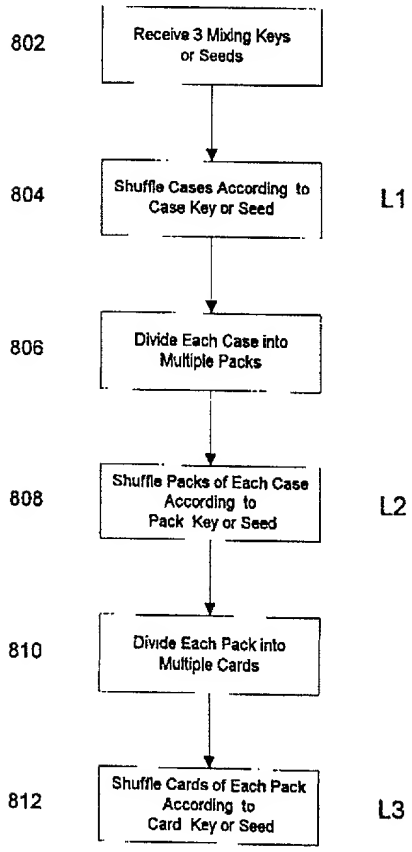


Fig. 9 Nested Shuffle of a Series of Cards

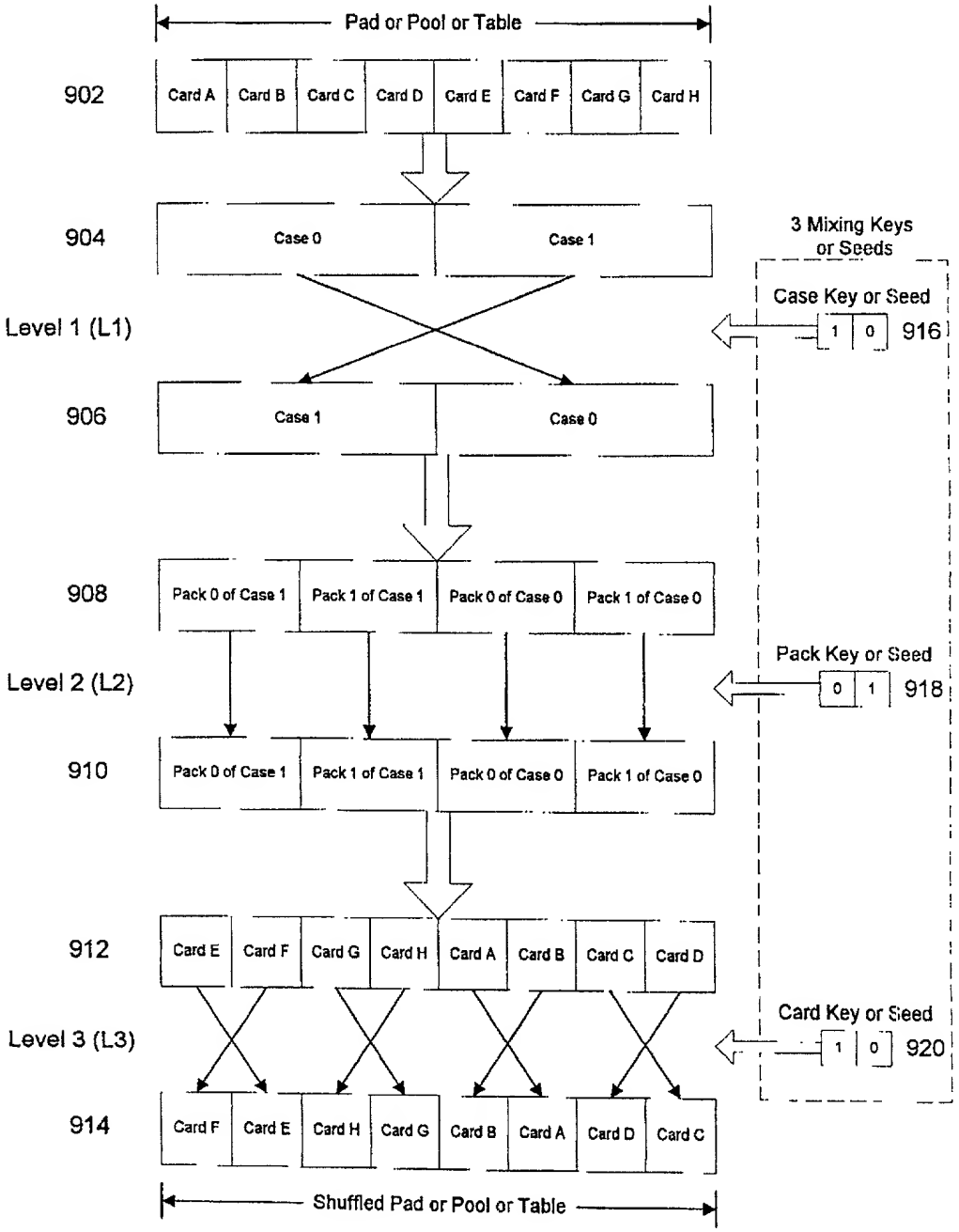


Fig. 10 Non-Cyclic Pseudo-Random Number Generator

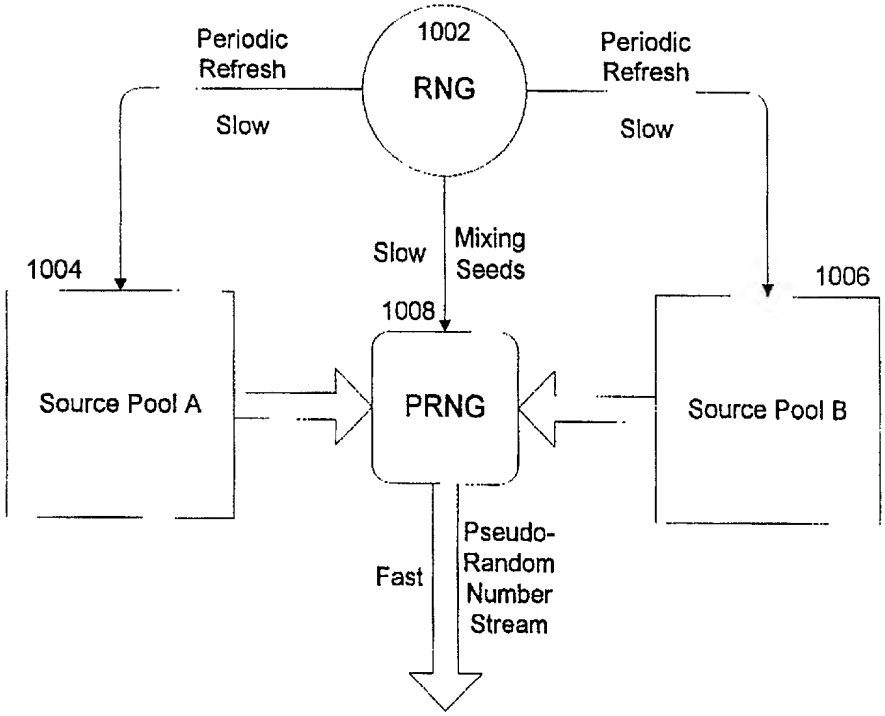


Fig. 11 Non-Cyclic Pseudo-Random Number Generation

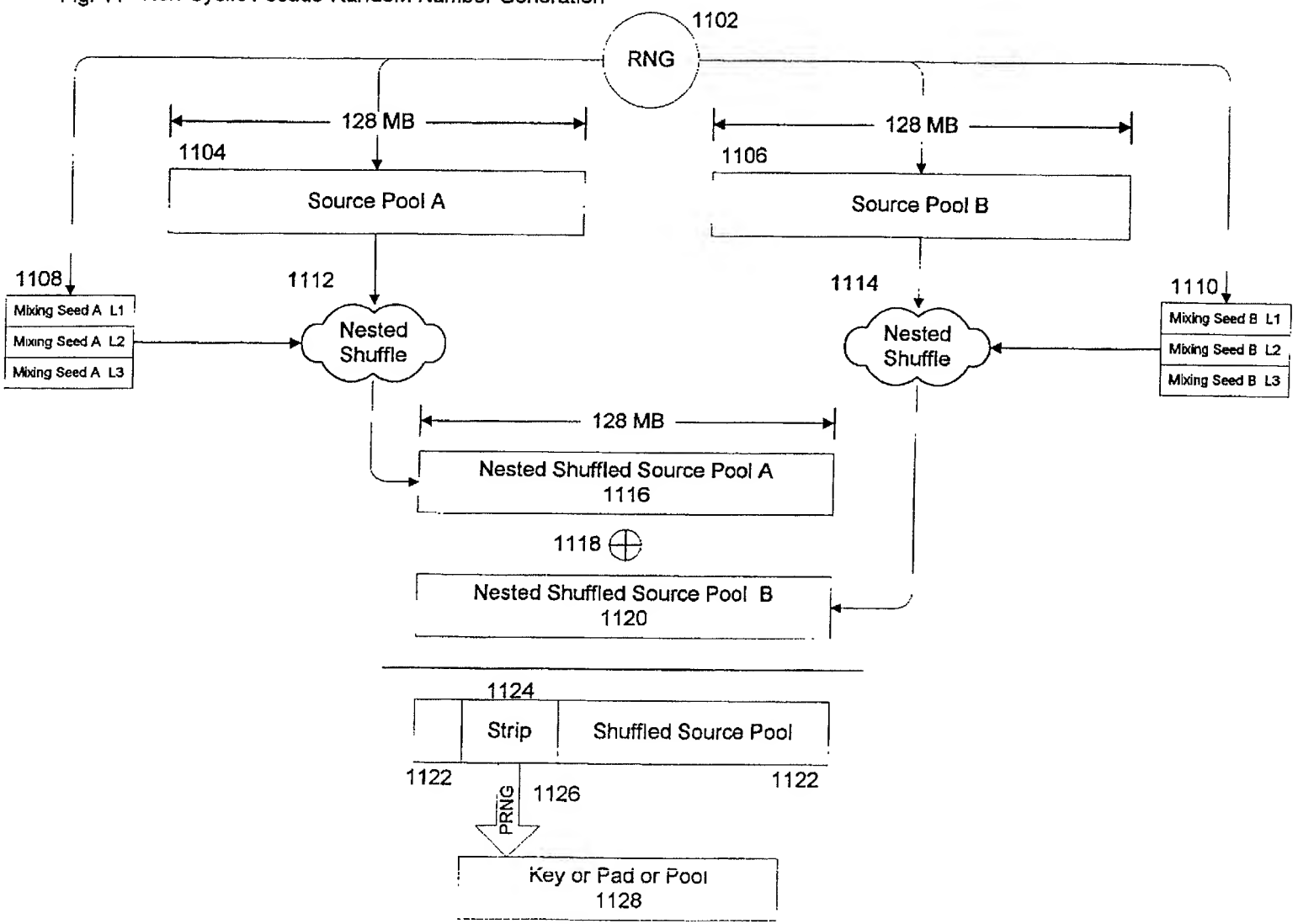


Fig. 12 N[illegible]d Shuffle of A Source Pool A or B [illegible]8 MB)

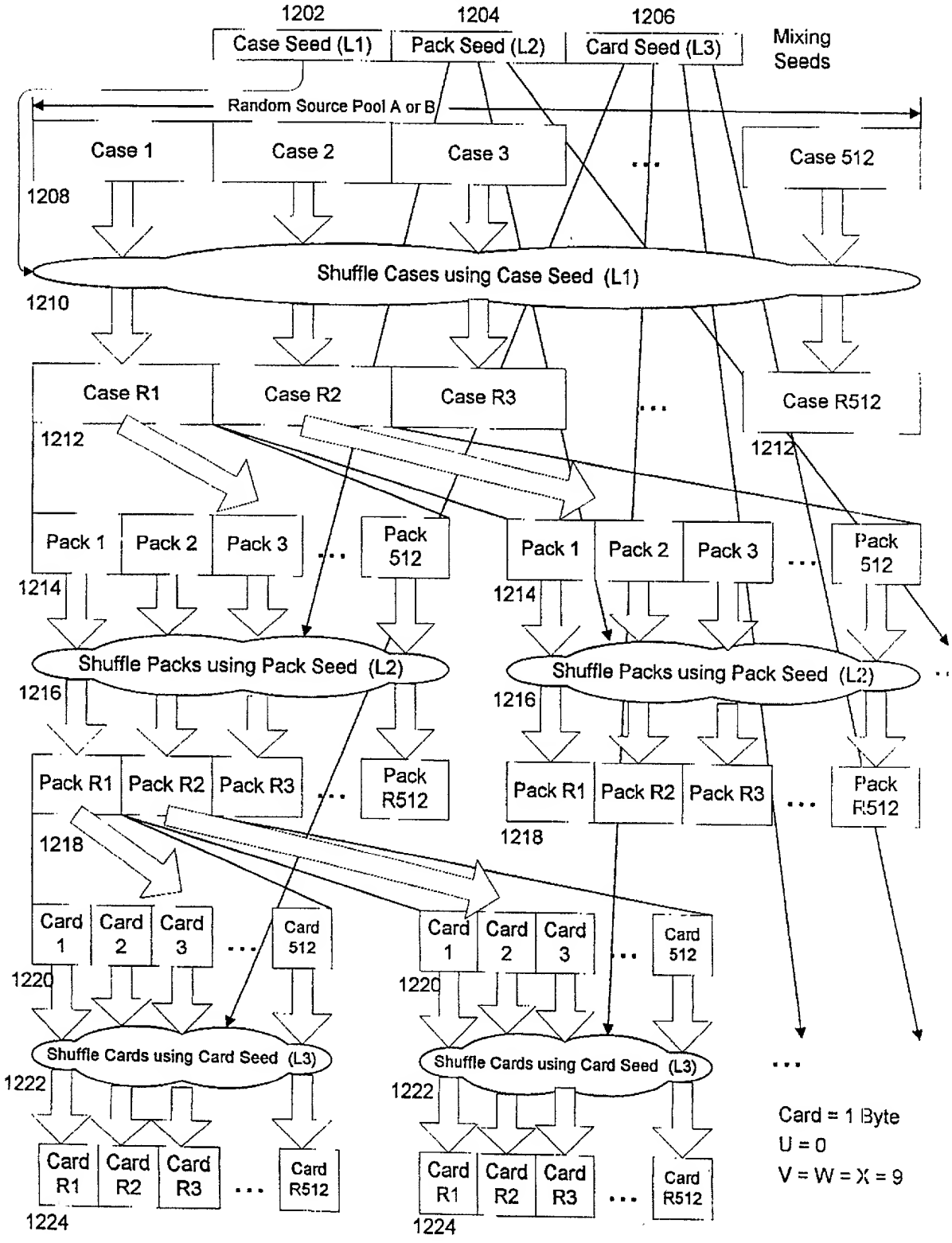


Fig. 13

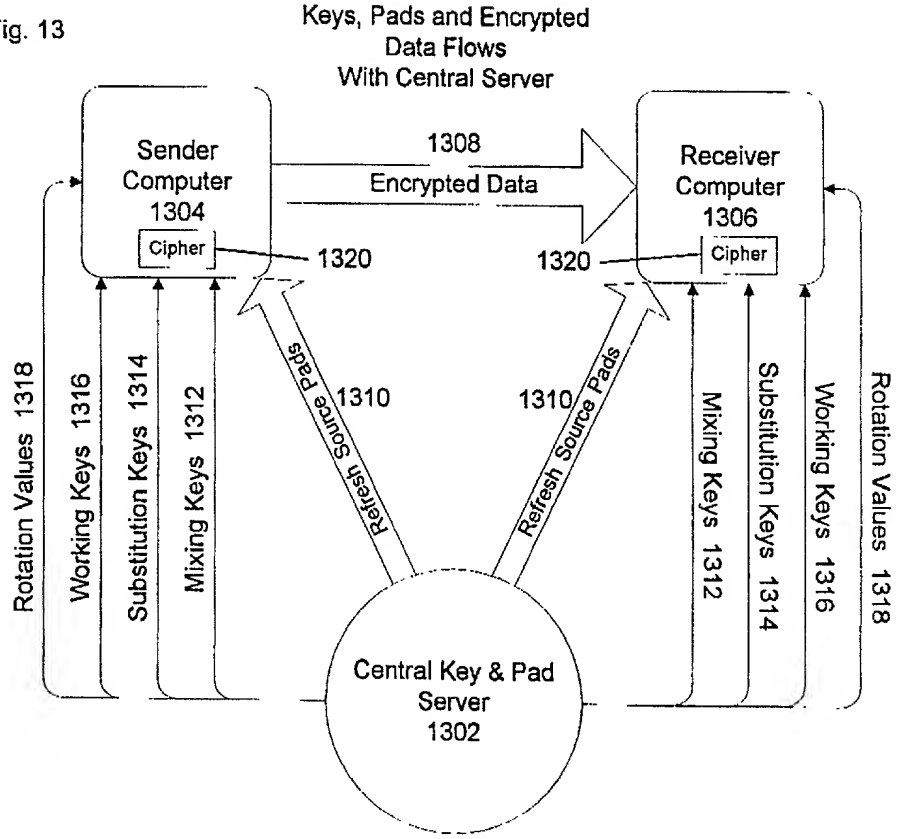

Keys, Pads and Encrypted Data Flows With Central Server
Sender Computer 1304
Cipher
1320
1308
Encrypted Data
Receiver Computer 1306
Cipher
1320
Rotation Values 1318
Working Keys 1316
Substitution Keys 1314
Mixing Keys 1312
1310
Refresh Source Pads
1310
Refresh Source Pads
Mixing Keys 1312
Substitution Keys 1314
Working Keys 1316
Rotation Values 1318
Central Key & Pad Server 1302

Fig. 14

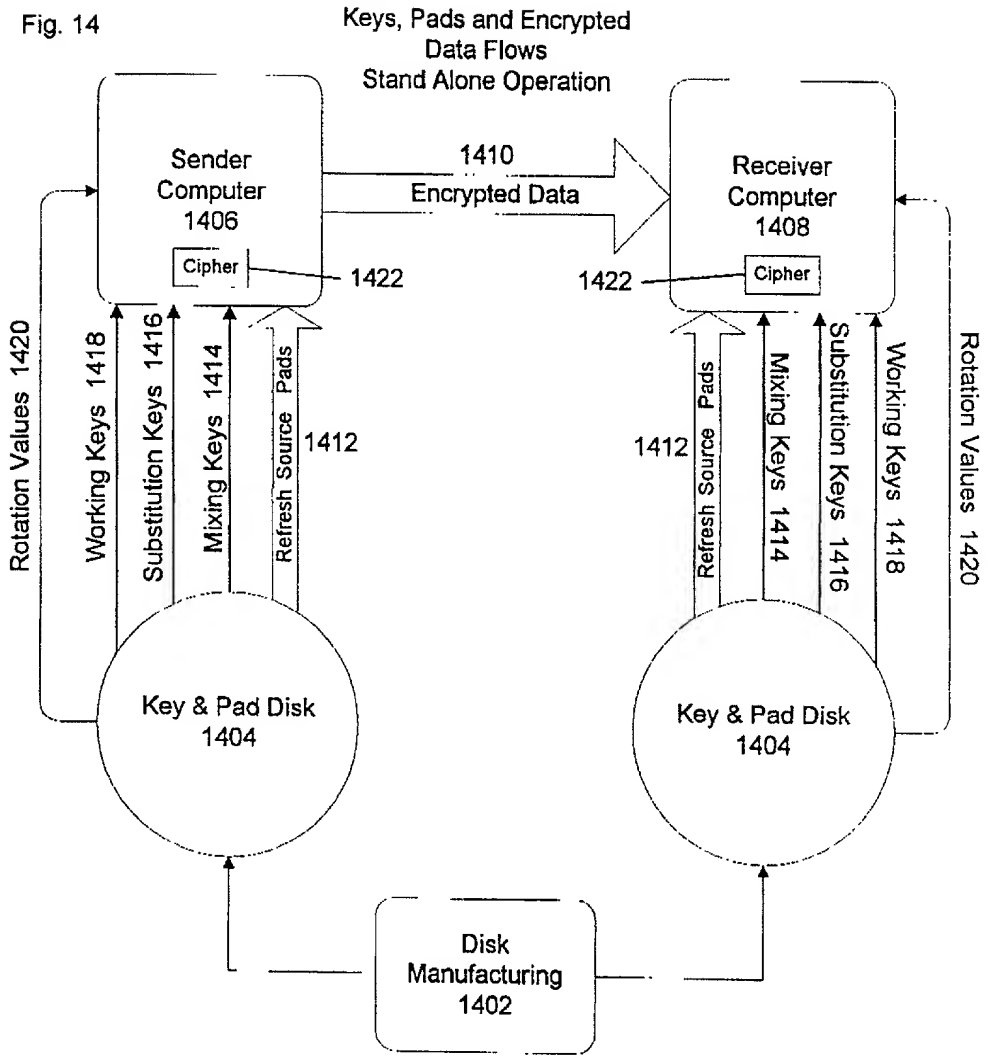

Keys, Pads and Encrypted
Data Flows
Stand Alone Operation
Sender
Computer
1406
Cipher
1422
1410
Encrypted Data
Receiver
Computer
1408
Cipher
1422
Rotation Values 1420
Working Keys 1418
Substitution Keys 1416
Mixing Keys 1414
Refresh Source Pads
1412
1412
Refresh Source Pads
Mixing Keys 1414
Substitution Keys 1416
Working Keys 1418
Rotation Values 1420
Key & Pad Disk
1404
Key & Pad Disk
1404
Disk
Manufacturing
1402

Fig. 15

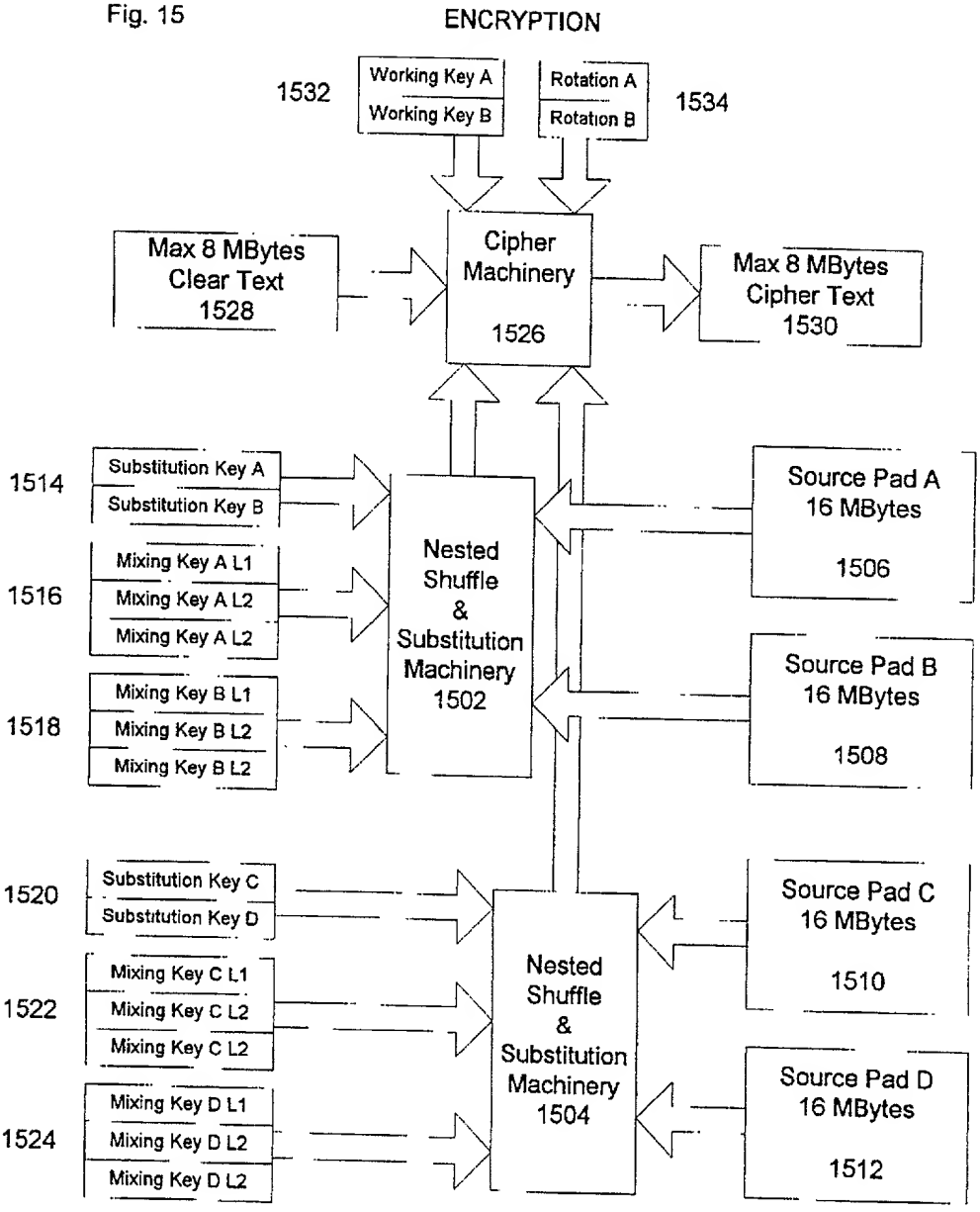

ENCRYPTION
1532
Working Key A
Working Key B
Rotation A
Rotation B
1534
Max 8 MBytes
Clear Text
1528
Cipher
Machinery
1526
Max 8 MBytes
Cipher Text
1530
1514
Substitution Key A
Substitution Key B
1516
Mixing Key A L1
Mixing Key A L2
Mixing Key A L2
1518
Mixing Key B L1
Mixing Key B L2
Mixing Key B L2
Nested
Shuffle
&
Substitution
Machinery
1502
Source Pad A
16 MBytes
1506
Source Pad B
16 MBytes
1508
1520
Substitution Key C
Substitution Key D
1522
Mixing Key C L1
Mixing Key C L2
Mixing Key C L2
1524
Mixing Key D L1
Mixing Key D L2
Mixing Key D L2
Nested
Shuffle
&
Substitution
Machinery
1504
Source Pad C
16 MBytes
1510
Source Pad D
16 MBytes
1512

Fig. 16 DECRYPTION

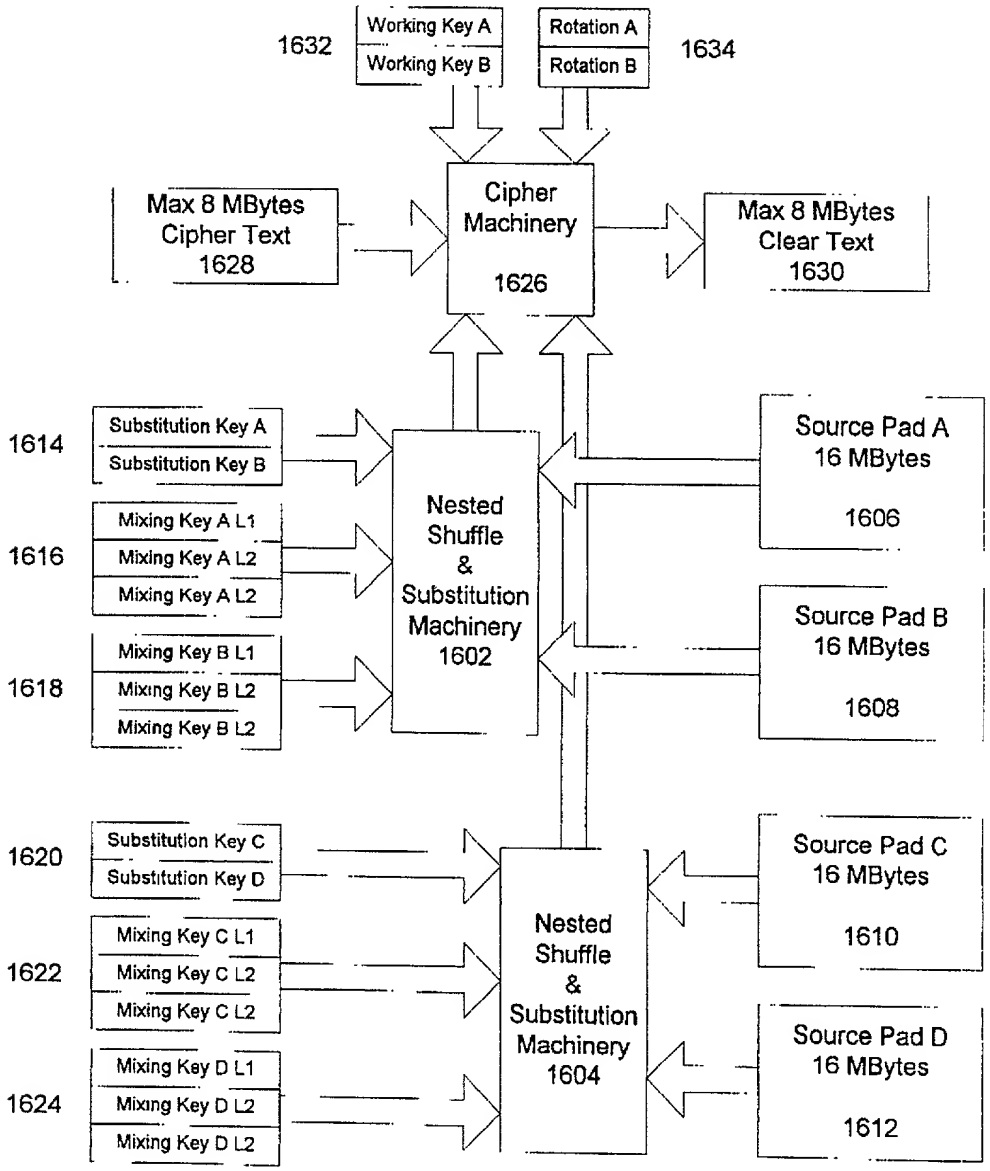


Fig. 17

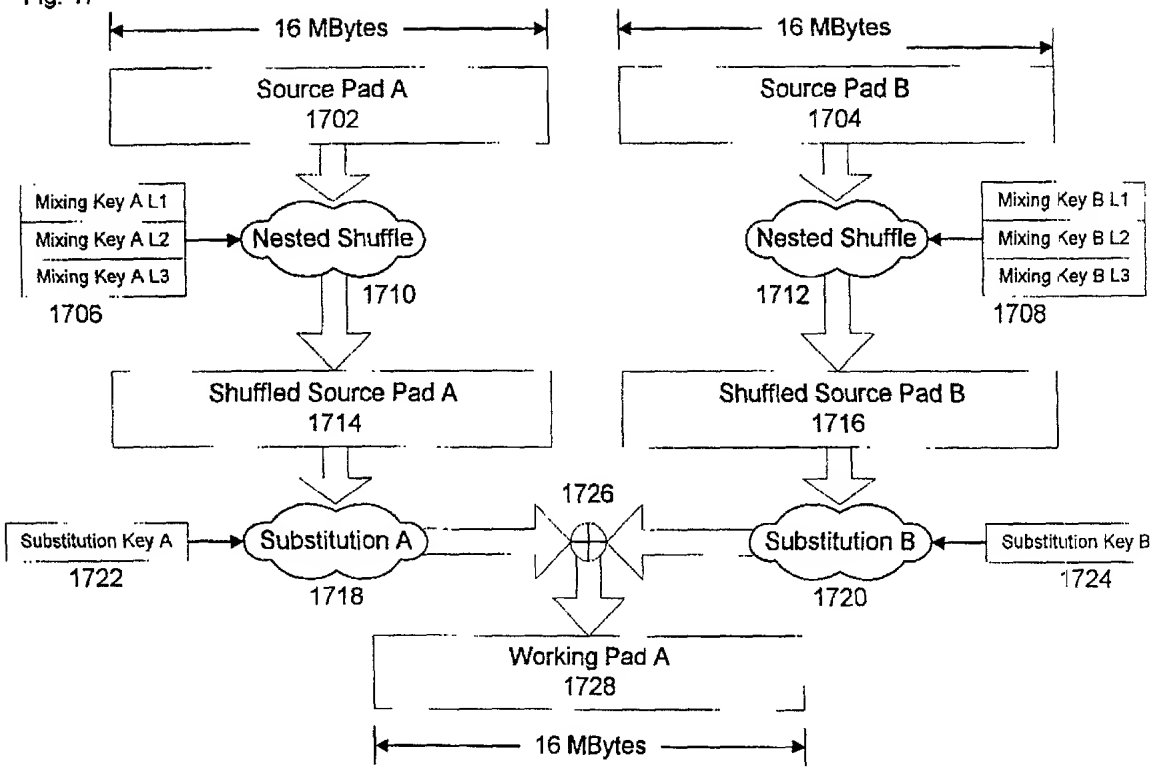

16 MBytes
16 MBytes
Source Pad A
1702
Source Pad B
1704
Mixing Key A L1
Mixing Key A L2
Mixing Key A L3
1706
Nested Shuffle
1710
Nested Shuffle
1712
Mixing Key B L1
Mixing Key B L2
Mixing Key B L3
1708
Shuffled Source Pad A
1714
Shuffled Source Pad B
1716
1726
Substitution Key A
1722
Substitution A
1718
Substitution B
1720
Substitution Key B
1724
Working Pad A
1728
16 MBytes

Fig. 18

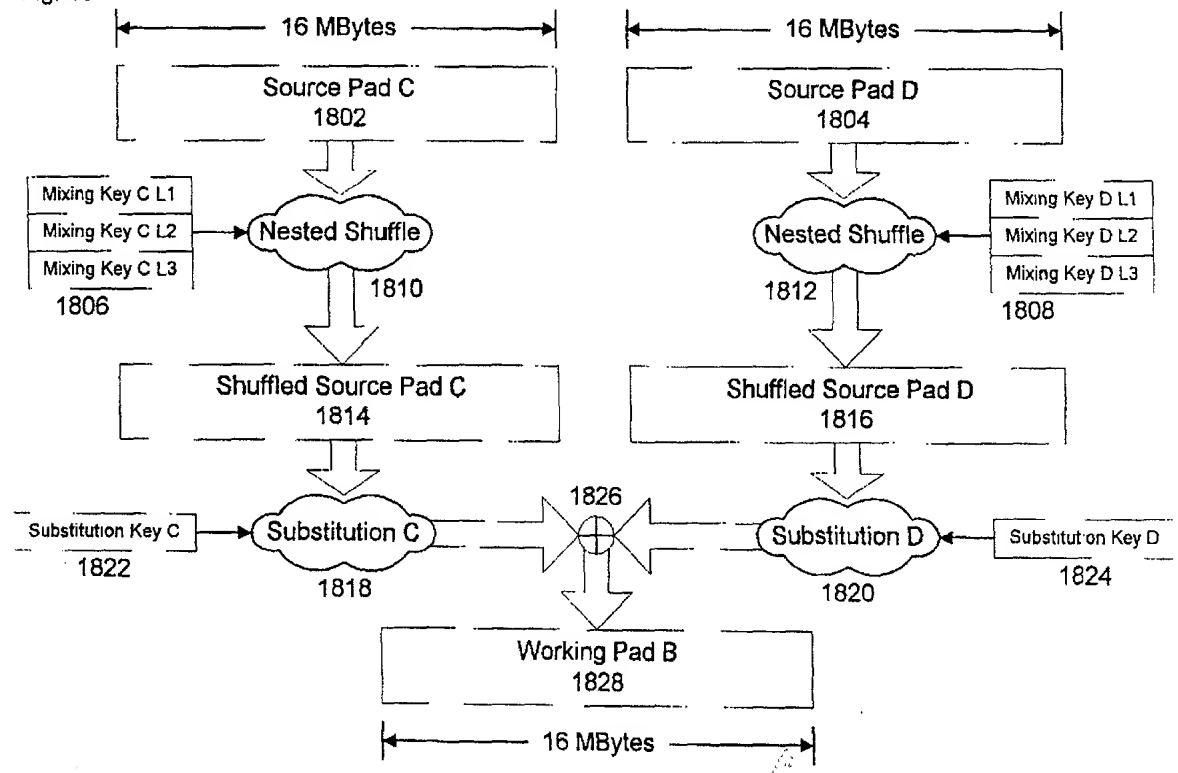

16 MBytes
16 MBytes
Source Pad C
1802
Source Pad D
1804
Mixing Key C L1
Mixing Key C L2
Mixing Key C L3
1806
Nested Shuffle
1810
Nested Shuffle
1812
Mixing Key D L1
Mixing Key D L2
Mixing Key D L3
1808
Shuffled Source Pad C
1814
Shuffled Source Pad D
1816
1826
Substitution Key C
1822
Substitution C
1818
Substitution D
1820
Substitution Key D
1824
Working Pad B
1828
16 MBytes

Fig. 19

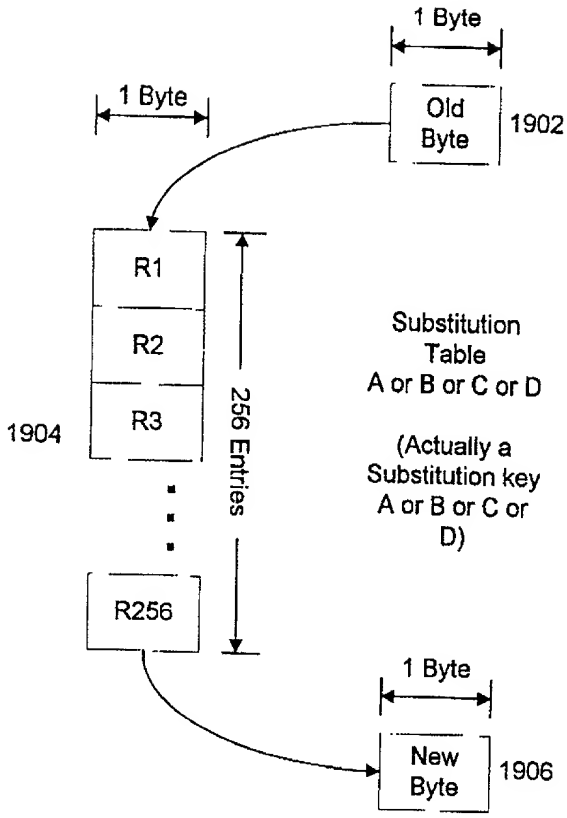

1 Byte
1 Byte
Old Byte
1902
R1
R2
R3
1904
256 Entries
R256
Substitution Table A or B or C or D
(Actually a Substitution key A or B or C or D)
1 Byte
New Byte
1906

Fig. 20

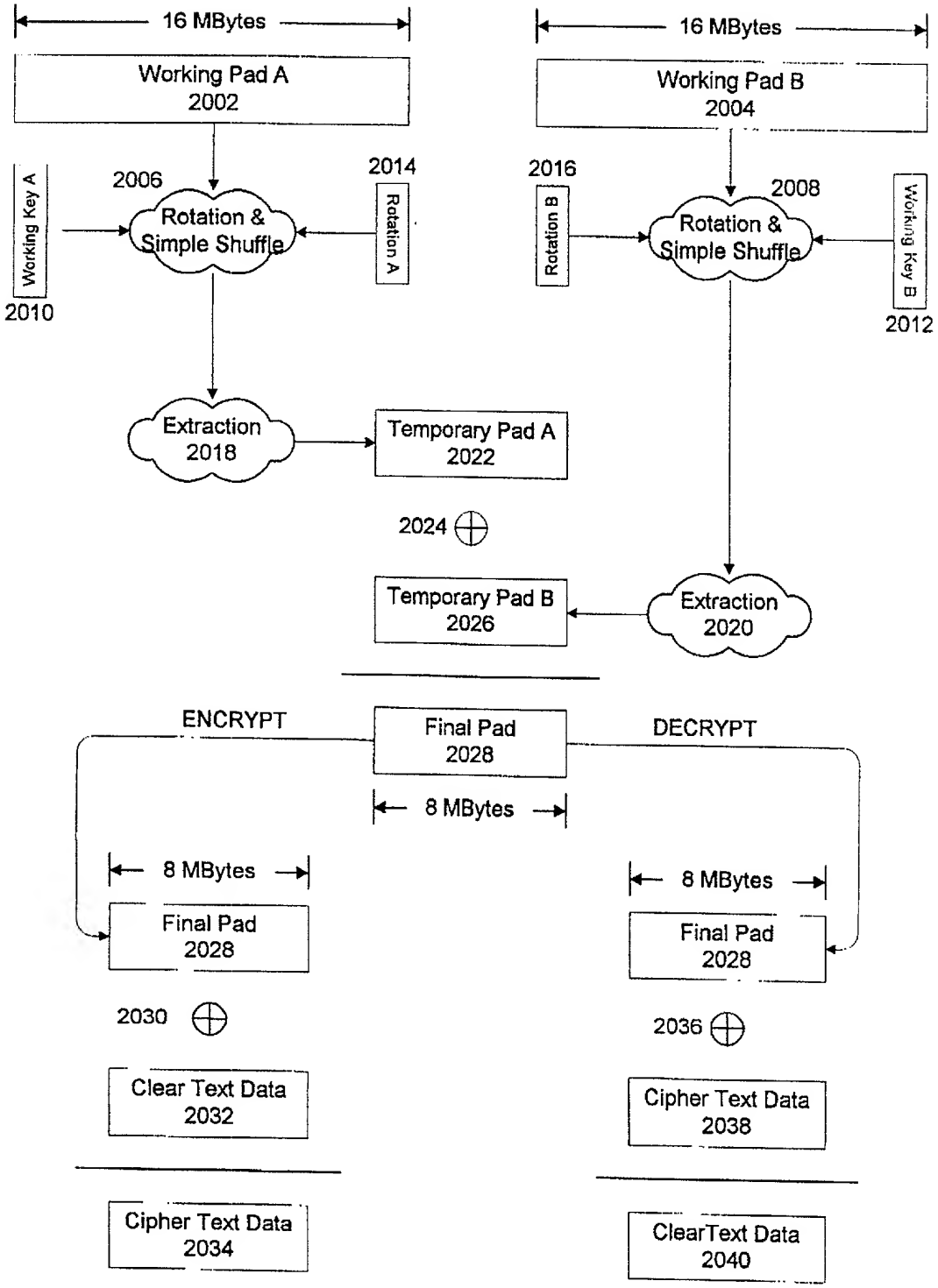

16 MBytes
Working Pad A
2002
16 MBytes
Working Pad B
2004
Working Key A
2006
Rotation &
Simple Shuffle
2014
Rotation A
2010
2016
Rotation B
2008
Rotation &
Simple Shuffle
Working Key B
2012
Extraction
2018
Temporary Pad A
2022
2024
Temporary Pad B
2026
Extraction
2020
ENCRYPT
Final Pad
2028
DECRYPT
8 MBytes
8 MBytes
8 MBytes
Final Pad
2028
Final Pad
2028
2030
2036
Clear Text Data
2032
Cipher Text Data
2038
Cipher Text Data
2034
ClearText Data
2040

Fig. 21 sted Shuffle Of A Source Pad (16 [illegible])

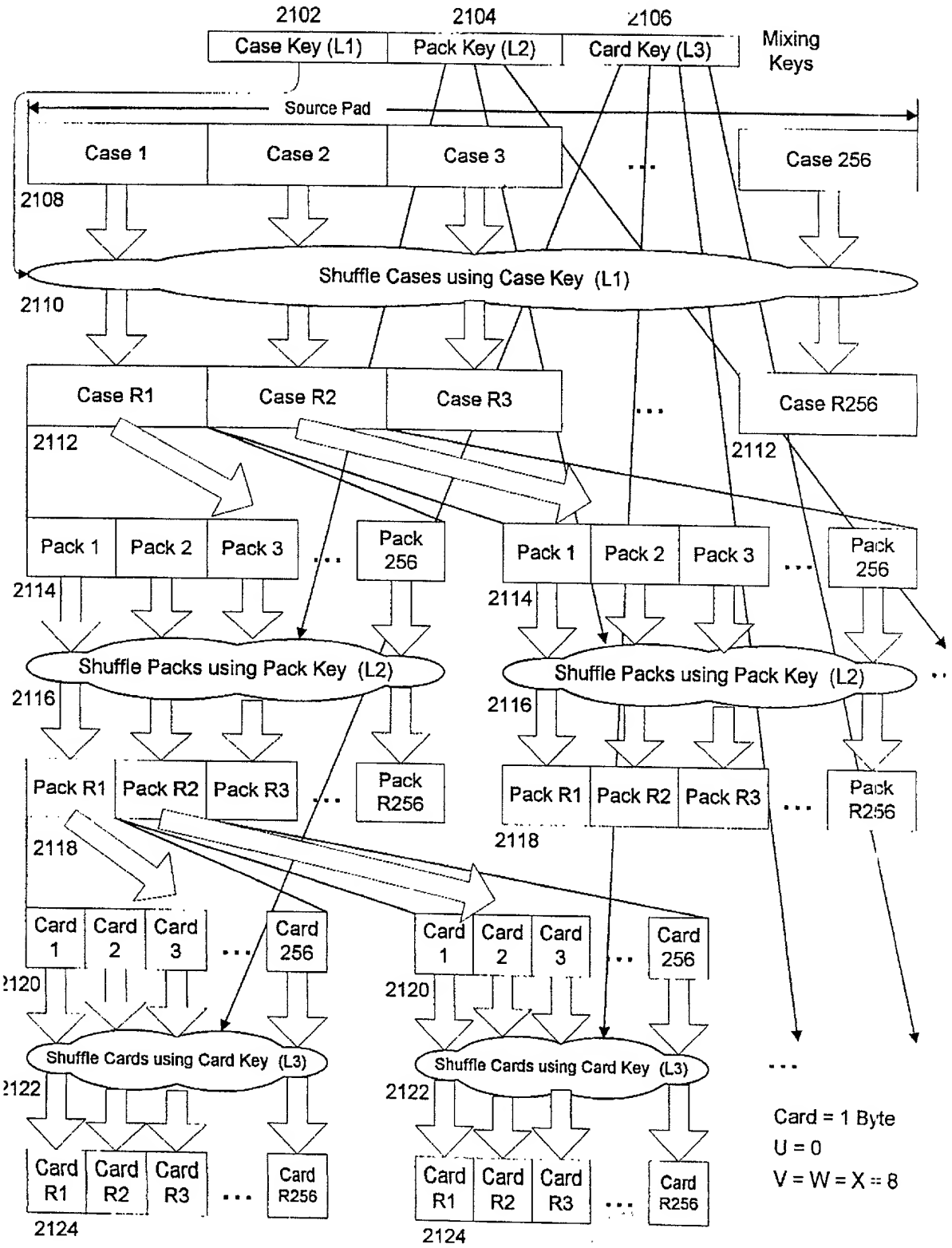


Fig. 22

Rotation & Simple Shuffle of Working Pad (16 MB)
and Extraction of a Temporary Pad (8MB)
Using a Working Key and Rotation Value

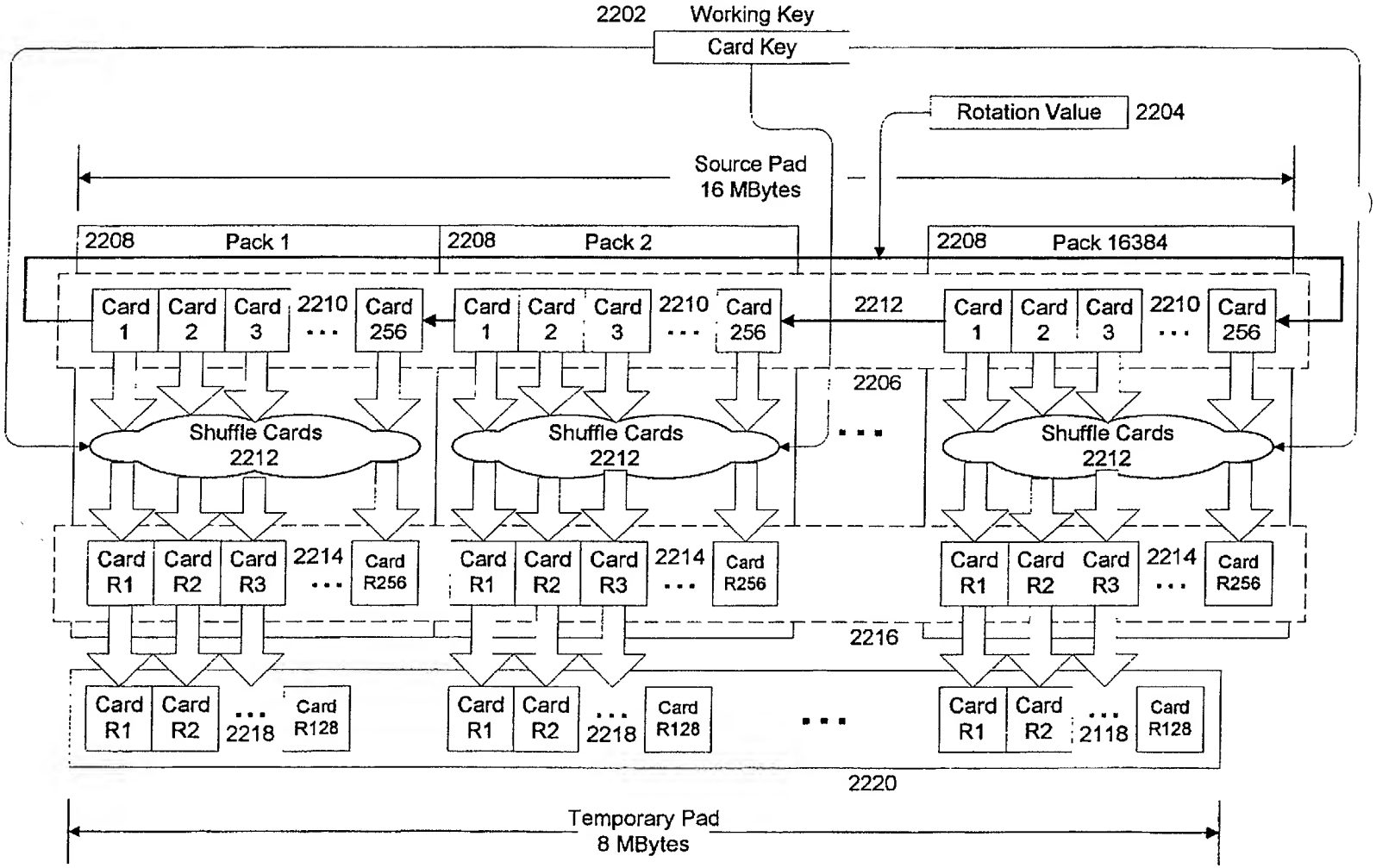


Fig. 23 Keyed One-Way Hash Function

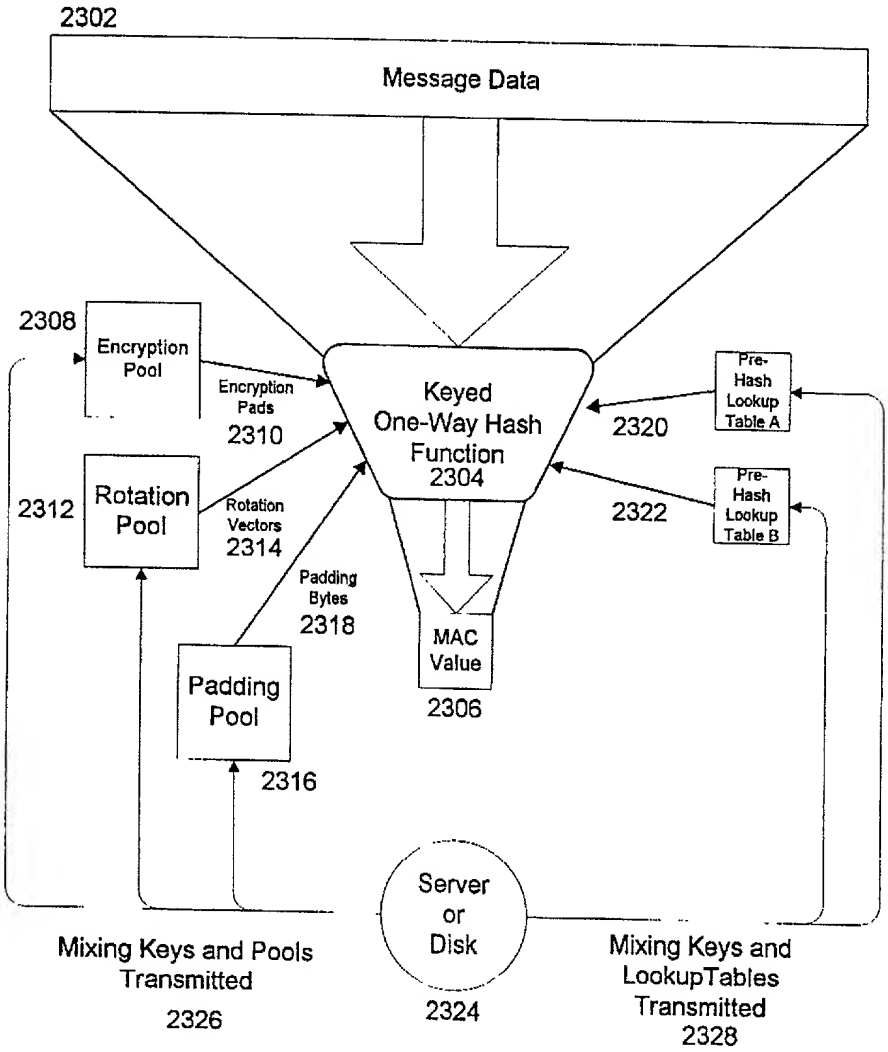


Fig. 24

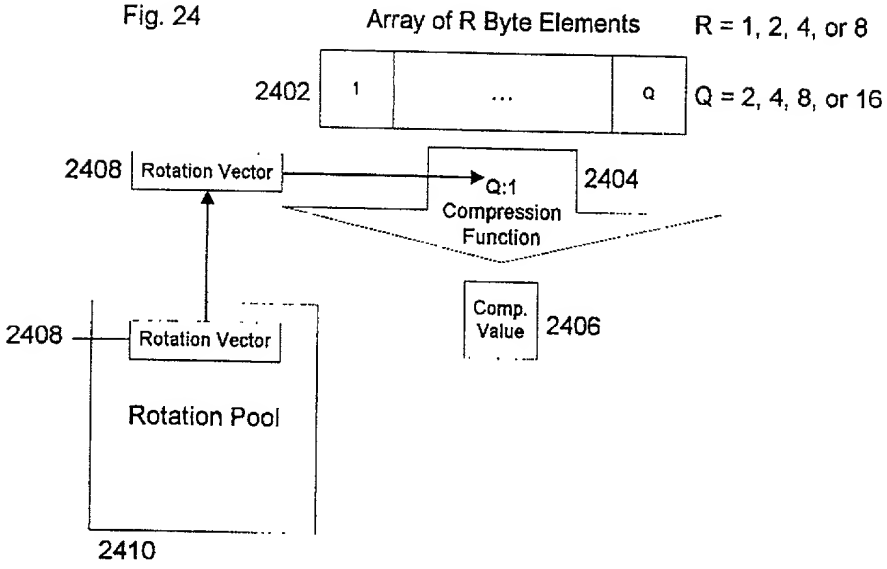

Array of R Byte Elements
R = 1, 2, 4, or 8
2402
1
...
Q
Q = 2, 4, 8, or 16
2408
Rotation Vector
Q:1
Compression
Function
2404
Comp.
Value
2406
2408
Rotation Vector
Rotation Pool
2410

Fig. 25

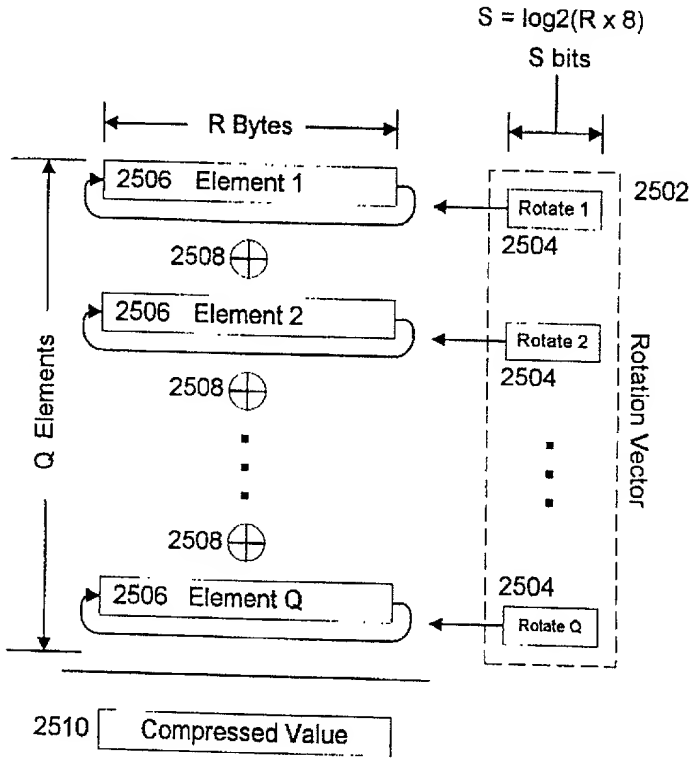

S = log2(R x 8)
S bits
R Bytes
2506 Element 1
Rotate 1
2502
2504
2508
2506 Element 2
Rotate 2
2504
2508
Q Elements
Rotation Vector
2508
2506 Element Q
2504
Rotate Q
2510
Compressed Value

Fig. 26

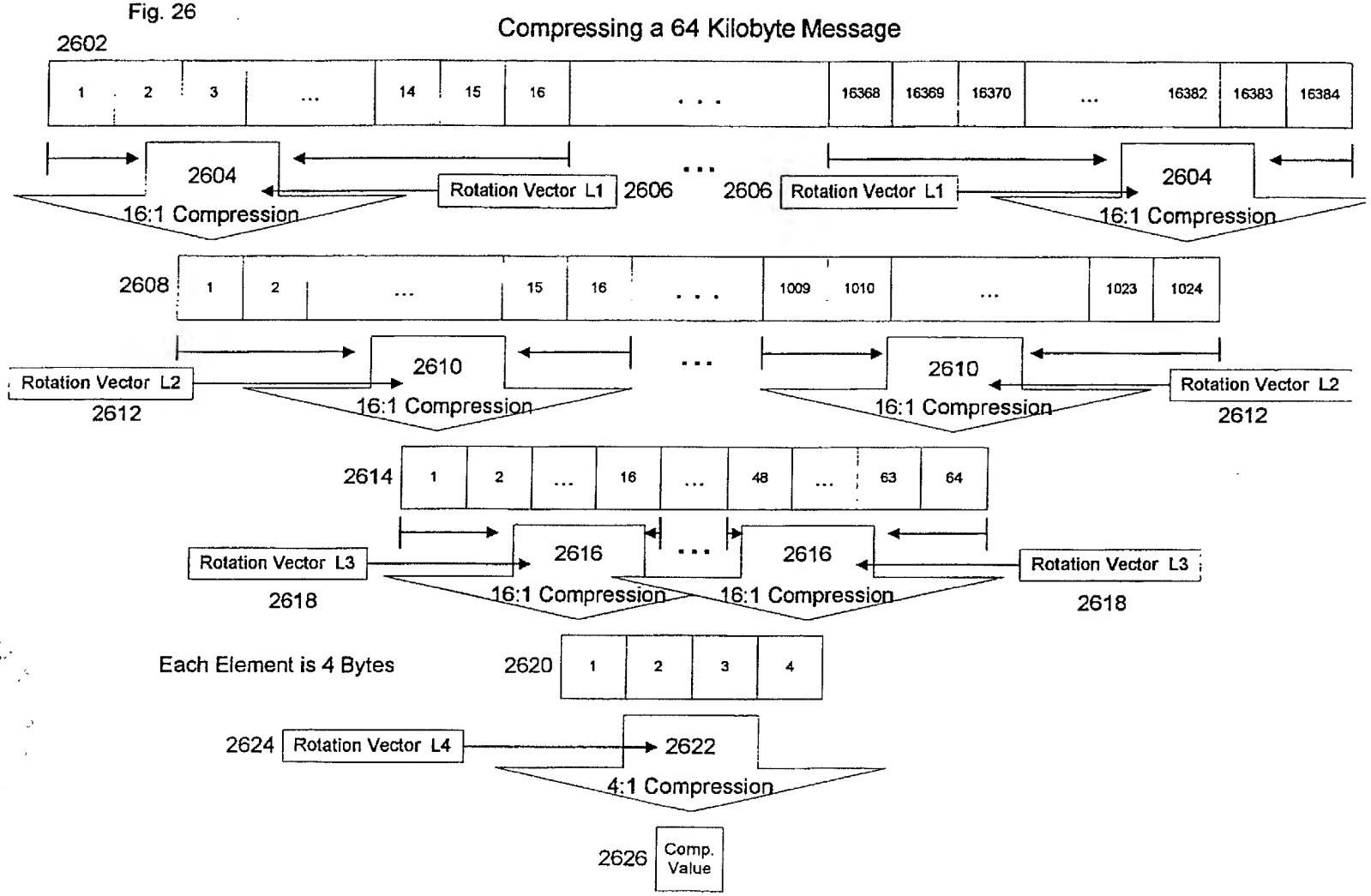

Compressing a 64 Kilobyte Message
2602
1
2
3
...
14
15
16
. . .
16368
16369
16370
...
16382
16383
16384
2604
16:1 Compression
Rotation Vector L1
2606
2606
Rotation Vector L1
2604
16:1 Compression
2608
1
2
...
15
16
. . .
1009
1010
...
1023
1024
Rotation Vector L2
2612
2610
16:1 Compression
2610
16:1 Compression
Rotation Vector L2
2612
2614
1
2
...
16
...
48
...
63
64
Rotation Vector L3
2618
2616
16:1 Compression
2616
16:1 Compression
Rotation Vector L3
2618
Each Element is 4 Bytes
2620
1
2
3
4
2624
Rotation Vector L4
2622
4:1 Compression
2626
Comp. Value

Fig. 27 Compressing a 64 Byte Message

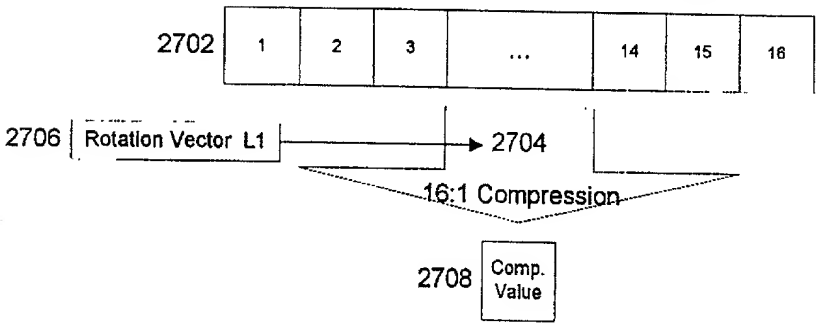


Fig. 28

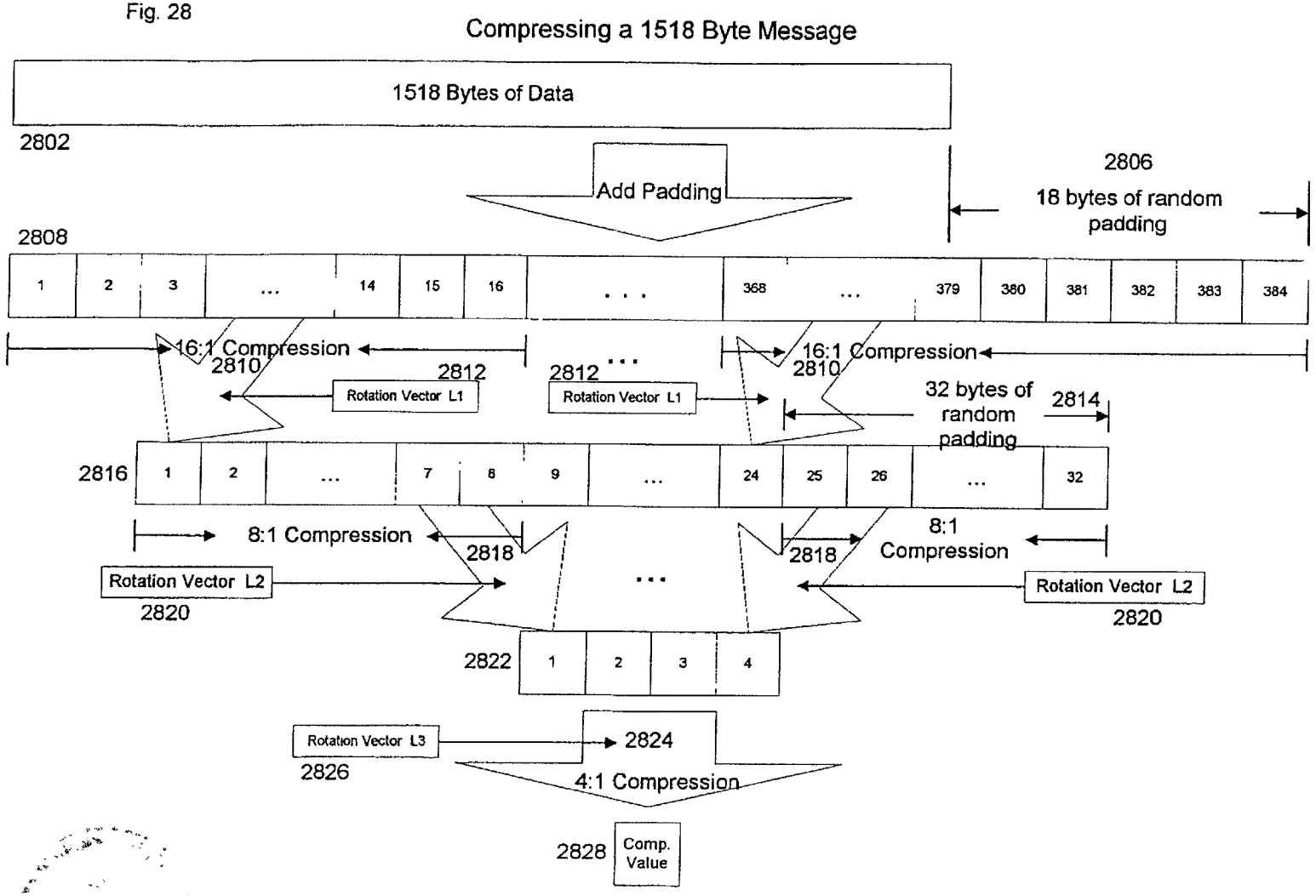

Compressing a 1518 Byte Message
1518 Bytes of Data
2802
Add Padding
2806
18 bytes of random padding
2808
1
2
3
...
14
15
16
. . .
368
...
379
380
381
382
383
384
16:1 Compression
2810
2812
Rotation Vector L1
2812
Rotation Vector L1
16:1 Compression
2810
32 bytes of random padding
2814
2816
1
2
...
7
8
9
...
24
25
26
...
32
8:1 Compression
2818
2818
8:1 Compression
Rotation Vector L2
2820
Rotation Vector L2
2820
2822
1
2
3
4
Rotation Vector L3
2826
2824
4:1 Compression
2828
Comp. Value

Fig. 29

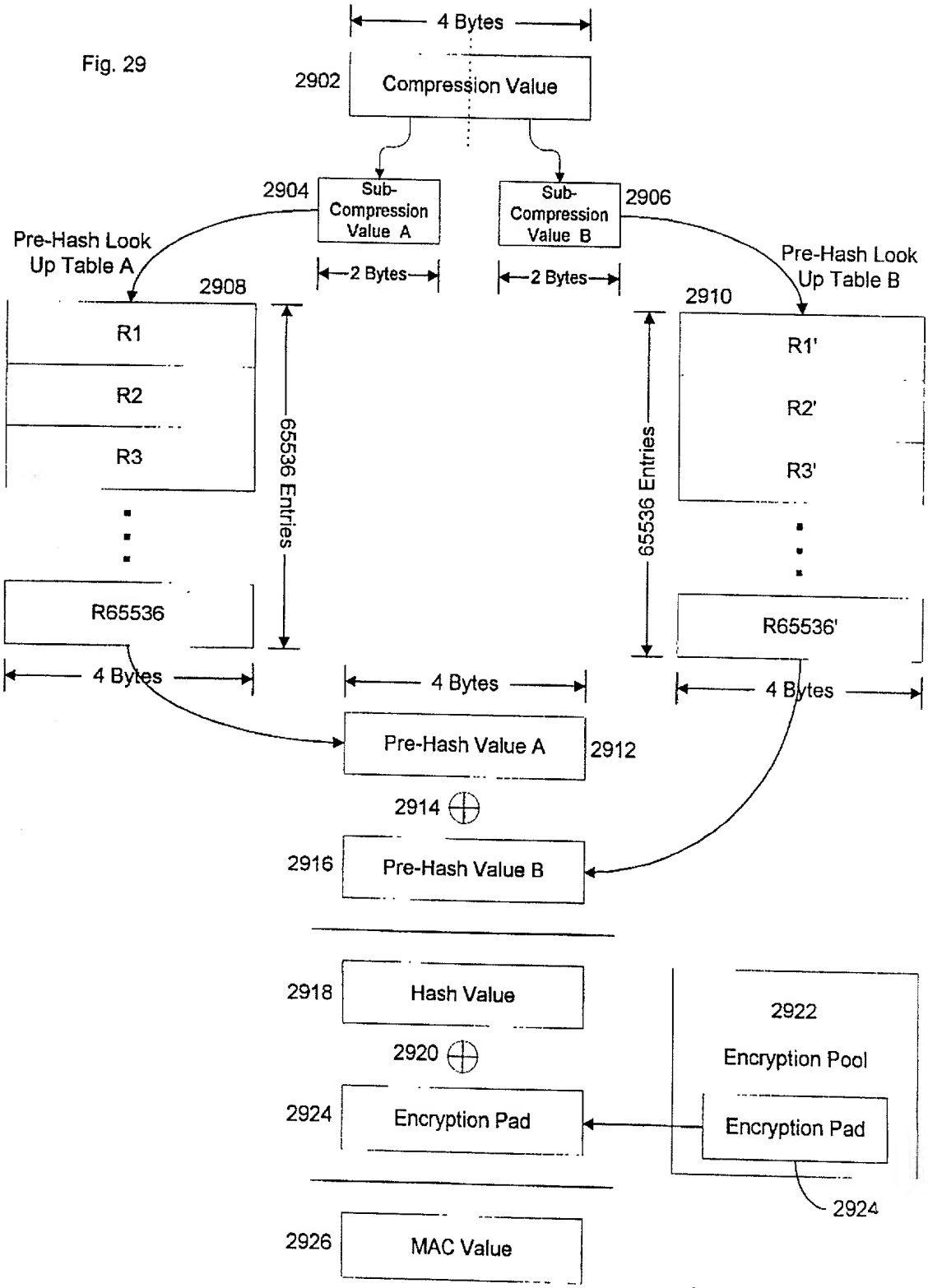

4 Bytes
2902
Compression Value
2904
Sub-Compression Value A
Sub-Compression Value B
2906
Pre-Hash Look Up Table A
Pre-Hash Look Up Table B
2908
2910
2 Bytes
2 Bytes
R1
R2
R3
R65536
R1'
R2'
R3'
R65536'
65536 Entries
65536 Entries
4 Bytes
4 Bytes
4 Bytes
Pre-Hash Value A
2912
2914
2916
Pre-Hash Value B
2918
Hash Value
2920
2922
Encryption Pool
2924
Encryption Pad
Encryption Pad
2924
2926
MAC Value

Fig. 30

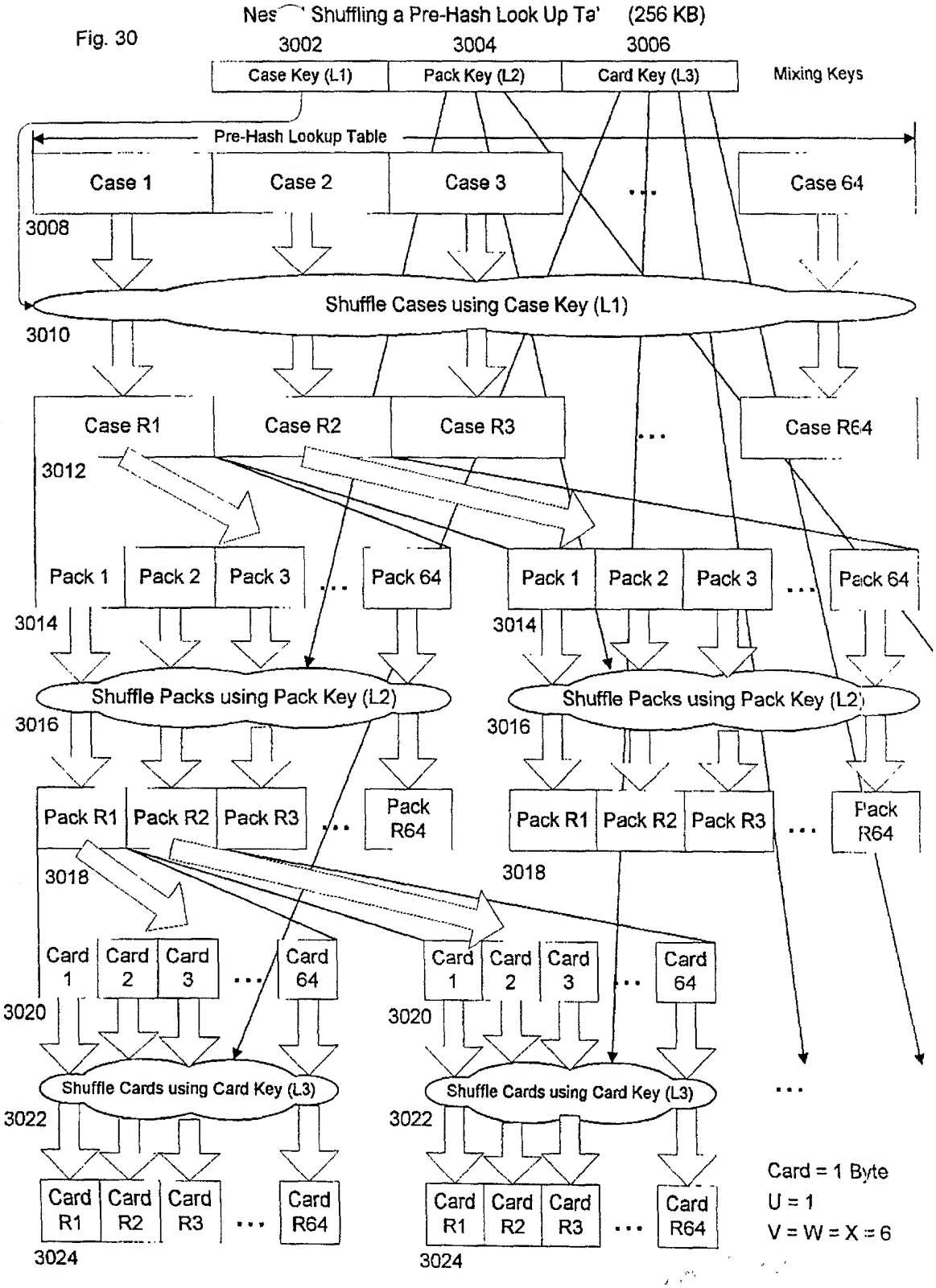

Nes Shuffling a Pre-Hash Look Up Ta (256 KB)
3002
3004
3006
Case Key (L1)
Pack Key (L2)
Card Key (L3)
Mixing Keys
Pre-Hash Lookup Table
Case 1
Case 2
Case 3
Case 64
3008
Shuffle Cases using Case Key (L1)
3010
Case R1
Case R2
Case R3
Case R64
3012
Pack 1
Pack 2
Pack 3
Pack 64
3014
Shuffle Packs using Pack Key (L2)
3016
Pack R1
Pack R2
Pack R3
Pack R64
3018
Card 1
Card 2
Card 3
Card 64
3020
Shuffle Cards using Card Key (L3)
3022
Card R1
Card R2
Card R3
Card R64
3024
Card = 1 Byte
U = 1
V = W = X = 6

Fig. 31

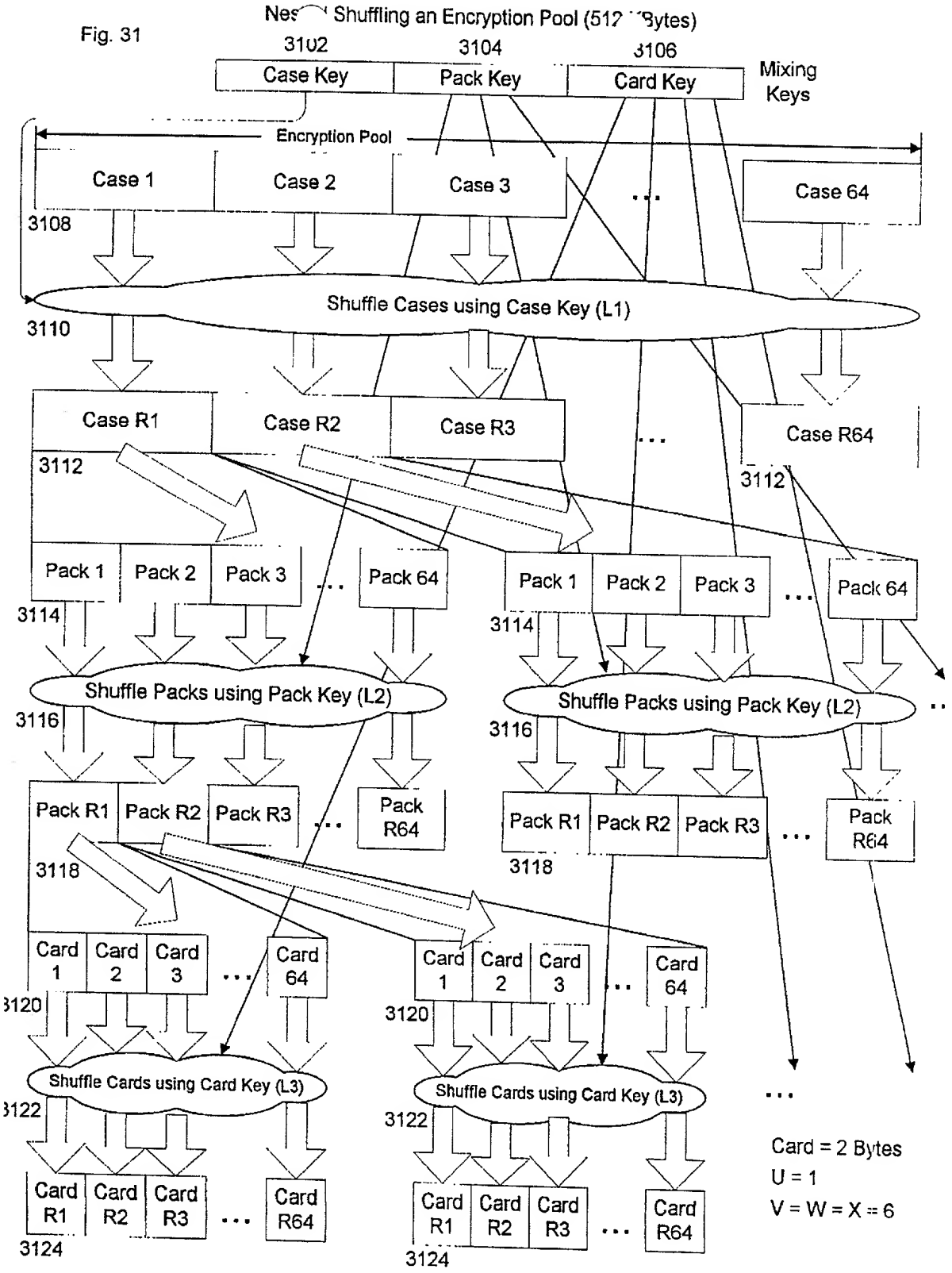

Nes Shuffling an Encryption Pool (512 Bytes)
3102
3104
3106
Case Key
Pack Key
Card Key
Mixing Keys
Encryption Pool
Case 1
Case 2
Case 3
Case 64
3108
Shuffle Cases using Case Key (L1)
3110
Case R1
Case R2
Case R3
Case R64
3112
Pack 1
Pack 2
Pack 3
Pack 64
3114
Shuffle Packs using Pack Key (L2)
3116
Pack R1
Pack R2
Pack R3
Pack R64
3118
Card 1
Card 2
Card 3
Card 64
3120
Shuffle Cards using Card Key (L3)
3122
Card R1
Card R2
Card R3
Card R64
3124
Card = 2 Bytes
U = 1
V = W = X = 6

Fig. 32

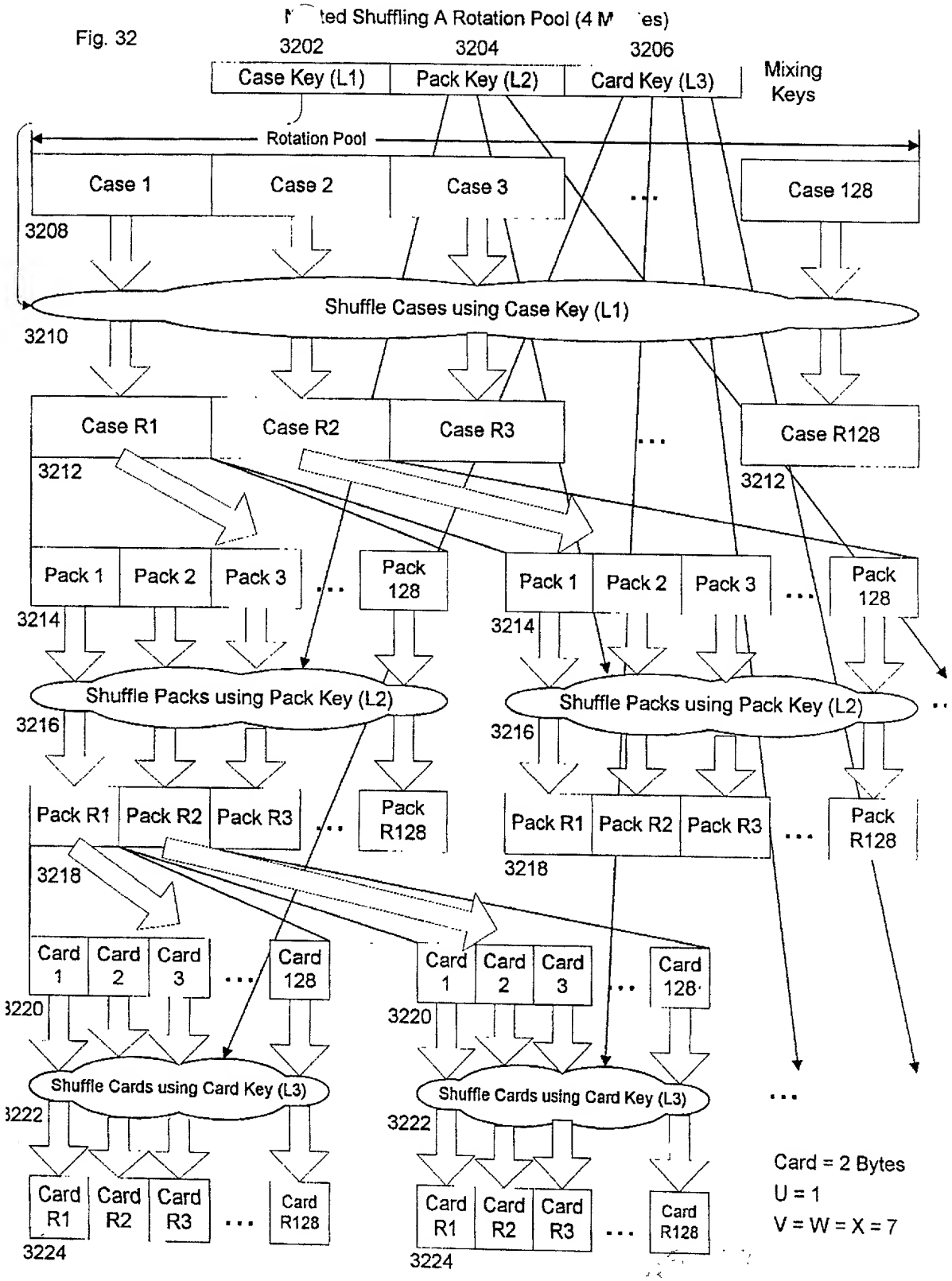

ted Shuffling A Rotation Pool (4 M es)
3202
3204
3206
Case Key (L1)
Pack Key (L2)
Card Key (L3)
Mixing Keys
Rotation Pool
Case 1
Case 2
Case 3
Case 128
3208
Shuffle Cases using Case Key (L1)
3210
Case R1
Case R2
Case R3
Case R128
3212
Pack 1
Pack 2
Pack 3
Pack 128
3214
Shuffle Packs using Pack Key (L2)
3216
Pack R1
Pack R2
Pack R3
Pack R128
3218
Card 1
Card 2
Card 3
Card 128
3220
Shuffle Cards using Card Key (L3)
3222
Card R1
Card R2
Card R3
Card R128
3224
Card = 2 Bytes
U = 1
V = W = X = 7

Fig. 33

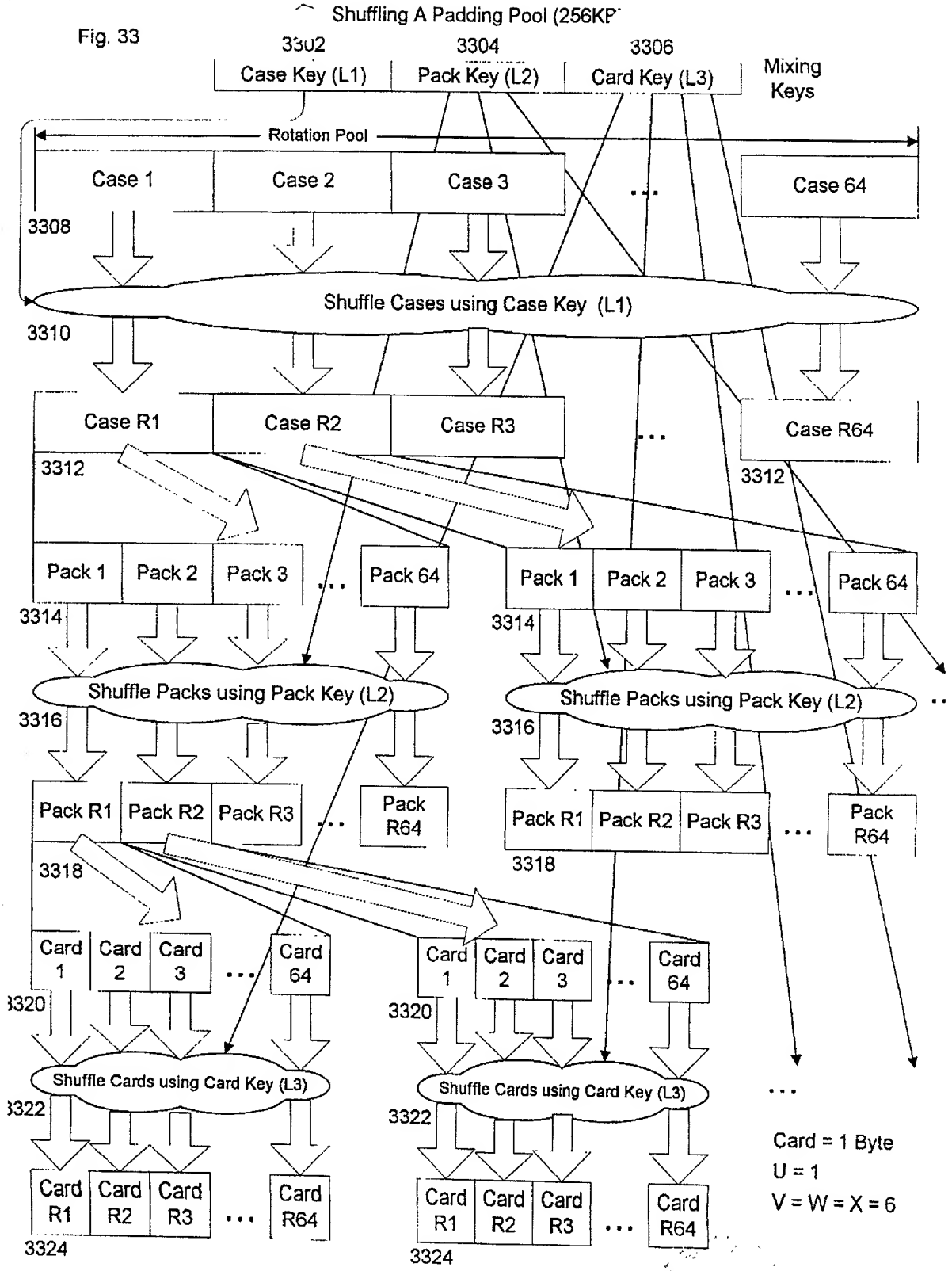
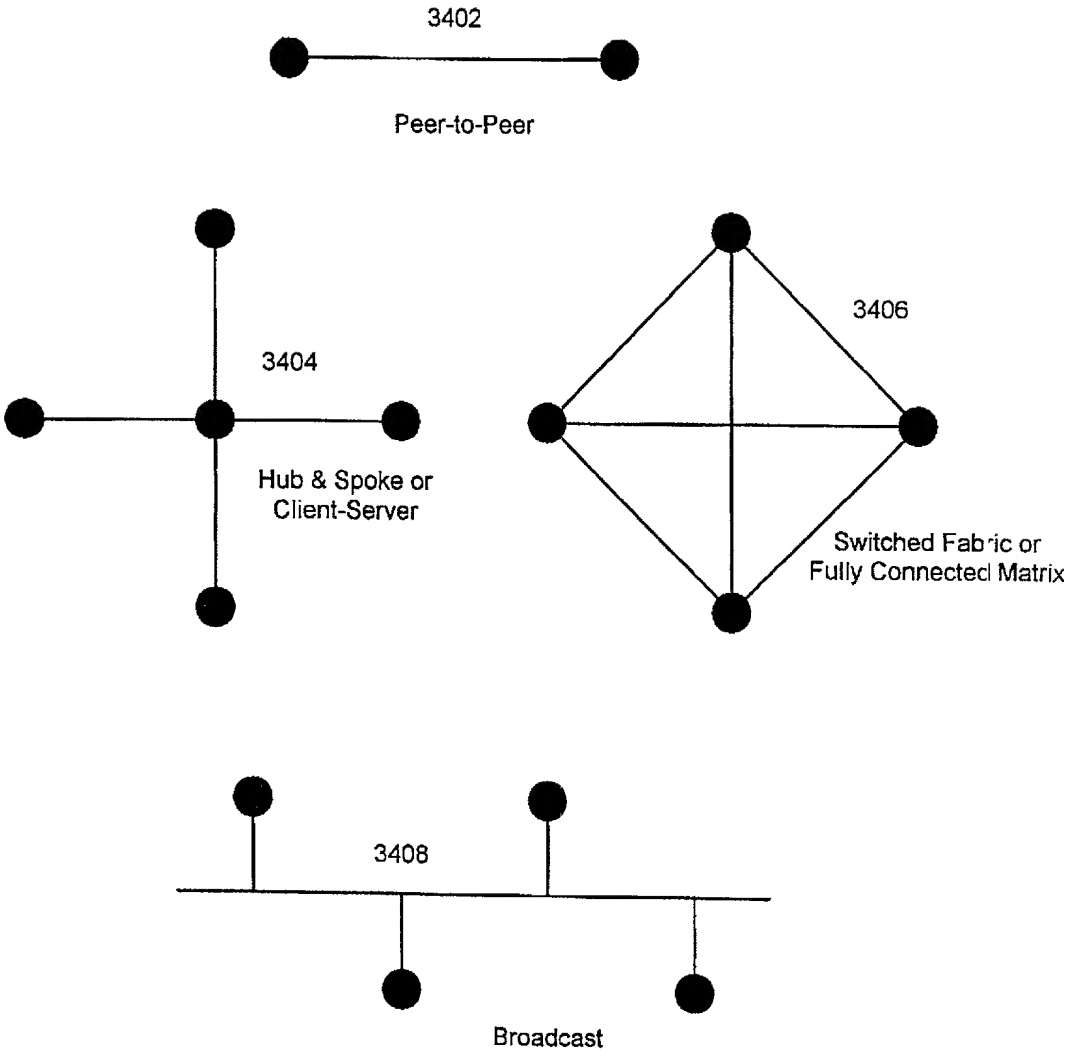

Shuffling A Padding Pool (256KP
3302
Case Key (L1)
3304
Pack Key (L2)
3306
Card Key (L3)
Mixing Keys
Rotation Pool
Case 1
Case 2
Case 3
Case 64
3308
Shuffle Cases using Case Key (L1)
3310
Case R1
Case R2
Case R3
Case R64
3312
Pack 1
Pack 2
Pack 3
Pack 64
3314
Shuffle Packs using Pack Key (L2)
3316
Pack R1
Pack R2
Pack R3
Pack R64
3318
Card 1
Card 2
Card 3
Card 64
3320
Shuffle Cards using Card Key (L3)
3322
Card R1
Card R2
Card R3
Card R64
3324
Card = 1 Byte
U = 1
V = W = X = 6

Fig. 34


3402
Peer-to-Peer
3404
Hub & Spoke or
Client-Server
3406
Switched Fabric or
Fully Connected Matrix
3408
Broadcast